**Как научить ребенка быть осторожным при знакомстве**

**с новыми людьми в Интернете**

 Общение в интернете может повлечь за собой коммуникационные риски, такие как не законные контакты ( например, груминг ), киберпреследования , кибербуллинг и др.

 Даже если у большинства пользователей чат-система добрые намеренья, среди них могут быть и злоумышленники. В некоторых случаях они хотят обманом заставить детей выдать личные данные, такие как домашний адрес, телефон, пароли к персональным страницам в Интернете и др. В других случаях они могут оказать преступникам в поисках жертвы.

Специалисты используют специальный термин « груминг», обозначающий установление дружеских отношений с ребенком с целью вступления в сексуальный контакт. Знакомство чаще всего происходит в чате, на форуме или в социальной сети от имени ровесника ребенка. Общаясь лично, злоумышленник входит в доверие к ребенку, пытается узнать личную информацию и договориться о встрече.

 **Предупреждение груминг:**

Будьте в курсе, с кем контактирует в Интернете ваш ребенок, старайтесь регулярно проверять список контактов своих детей, чтобы убедиться, что они лично знают всех, с кем они общаются;

Объясните ребенку, что нельзя разглашать в Интернете информацию личного характера, а также пересылать интернет-знакомым свои фотографии;

 Если ребенок интересуется контактами с людьми намного старше его, следует провести разъяснительную беседу;

Не позволяйте вашему ребенку встречаться с онлайн-знакомыми без вашего разрешения или в отсутствии взрослого человека. Если ребенок желает встретиться с новым интернет-другом, следует настоять на сопровождении ребенка на эту встречу;

Интересуйтесь тем, куда и с кем ходит ваш ребенок.

**Как избежать кибергуллинга**

 Кибергуллинг - преследование сообщениями, содержащими оскорбления, агрессию, запугивание; социальное бойкотирование с помощью различных интерне-серверов.

Предупреждение кибербуллинга;

 Объясните детям, что при общении в Интернете они должны быть дружелюбными с другими пользователями. Ни в коем случае не писать грубых слов – читать грубости также неприятно. Как и слышать;

Научите детей правильно реагировать на обидные слова или действия других пользователей;

Объясните детям, что нельзя использовать сеть для хулиганства, распространения сплетен или угроз;

Стварайтесь следить за тем, что ваш ребенок делает в Интернете, а также следите за его настроением после пользования сетью.

Даже при самых доверительных отношениях в семье родители иногда не могут вовремя заметить грозящую ребенку опасность и, тем более, не всегда знают как ее предотвротить.

Родиделям следует обротить внимание на ряд призноков в поведении ребенка, которие могут свидетельствовать о том, что ребенок стал жертвой кибербулинга;

*Беспокойное поведение*

Даже самый замкнутый школьник будет переживать из-за происходящего и обязательно выдаст себя своим поведением. Депрессия и не желание идти в школу - самые явные признаки того, что ребенок подвергается агрессии.

 *Неприязнь к Интернету*

 Если ребенок любит проводить время в интернете и внезапно перестал это делать, следует выяснить причину. В очень редких случаях детям действительно надоедает проводить время в сети. Однако в большинстве случаев внезапное нежелание пользоваться Интернетом связано с проблемами в виртуальном мире.

*Нервозность при получении новых сообщений*

Негативная реакция ребенка на звуки письма на электронную почту должна насторожить родителя. Если ребенок регулярно получает сообщения, которые расстраивают его. Поговорите с ним и обсудите содержание этих сообщений.

**Как научить ребенка быть осторожным в Сети и не стать жертвой интернет-мошенников**

Кибермошенничество – один из видов киберпреступления, целью которого является обман пользователей: незаконное получение доступа либо хищение личной информации, с целью причинить материальные или иной ущерб.

Предупреждение кибермошенничества:

 Проинформируйте ребенка о самых распространенных методах мошенничества и научите его советоваться с взрослыми перед тем, как воспользоваться теми или иными услугами в интернете;

Установите на свои компьютеры антивирус или. Например. Персональный брандмауэр. Эти приложения наблюдают за трафиком и могут быть использованы для выполнения множества действий на зараженных системах, наиболее частым из которых являются кража конфиденциальных данных.

**Безопасное совершение покупок в интернет-магазинах**

1. Прежде чем совершать покупку в интернет – магазине, удостоверьтесь в его надежности;

2. Необходимо вместе с ребенком познакомиться с отзывами покупателей;

3. Проверьте реквизиты и название юридического лица - владельца магазина;

4. Уточните, как долго существует магазин. Посмотреть можно в поисковике или по дате регистрации документа (сервис Whols)

5.Поинтерисуйтесь выдает ли магазин кассовый чек

6. Сравните цены в разных интернет – магазинах

 7.Позвоните в справочную магазина

8. Обратите внимание на правила интернет-магазина

9.Выясните, сколько точно вам придется заплатить

**Как распознать интернет - и игровую зависимость**

Сегодня все более актуальны проблемы так называемой «интернет – зависимости» и зависит от компьютерных игр. Первыми с ними столкнулись врачи-психотерапевты, а также компании, использующие в своей деятельности Интернет и несущие убытки, в случае если, если у сотрудников появляется патологическое влечение к пребыванию онлайн. Согласно исследованиям Кимберли Янг, предвестниками интернет зависимости являются:

1. Навязчивое стремление постоянно проверять электронную почту;

2. предвкушение следующего сеанса онлайн;

3. Увеличение времени, проводимого онлайн;

4. увеличении количество денег, расходуемых онлайн.

Если вы считаете, что ваши близкие, в этом числе дети, страдают от чрезмерной увлеченности компьютером, это наносит вред их здоровью, учебе, отношением в обществе, приводит к сильным конфликтом в семье, то вы можете обратиться к специалистом, занимающимся этой проблемой. Они помогут построить диалог и убедить зависимого признать существование проблемы и согласиться получить помощь.

 **Как научить ребенка не загружать на компьютер вредоносные программы**

Вредоносные программы могут нанести вред компьютеру и хранящимся на нем данным. Они также могут снижать скорость обмена данными и даже использовать ваш компьютер для распространения вируса, рассылать от вашего имени спам с адреса электронной почты или профиля какой-либо социальной сети.

**Предупреждения столкновения с вредоносными программами:**

Установите на все домашние компьютеры специальные почтовые фильтры и антивирусные системы для предотвращения заражения программного обеспечении и потере данных. Такие приложения наблюдают за трафиком и могут предотвратить как прямые атаки злоумышленников, таки атаки, использующие вредоносные приложения.

Используйте только лицензионные программы и данные, полученные из надежных источников. Чаще всего вирусами бывают заражены пиратские копии программ, особенно игр.

Объясните работу ребенка, как важно использовать только проверенные информационные ресурсы и не скачивать нелицензионный контент.

Периодически старайтесь полностью проверять свои домашние компьютеры.

 Делайте резервную копию важных данных.

Старайтесь периодически менять пороли и не используйте слишком простые пороли.

**Что делать, если ребенок всеже столкнулся с какими -либо рисками**

Установите положительный эмоциональный контакт с ребенком, расположите его к разговору о том, что случилось. Расскажите о своей обеспокоенности тем, что с ними происходит. Ребенок должен вам доверять и знать, что вы хотите разобраться в ситуации и помочь ему, а не наказать;

Посторайтесь внимательно выслушать рассказ о том, что произошло, понять насколько серьезно произошедшее и насколько серьезно это могло повлиять на ребенка;

Если ребенок расстроен чем-то увиденный, или он попал в неприятную ситуацию-посторайтесь его успокоить и вместе с ними разберитесь в ситуации- что привело к данному результату, какие неверные действия совершил сам ребенок. А где вы не рассказали ему о правилах безопасности в интернете;

Если ситуация связана с насилием в интернете по отношению к ребенку, то необходимо выяснить информацию об агрессоре, выяснить историю взаимоотношений ребенка и агрессора, выяснить существует ли договоренность о встрече в реальной жизни; узнать были ли такие встречи и что известно агрессору о ребенке, жестко настаивайте на избегание встреч с незнакомцами, особенно без свидетелей, проверьте все новые контакты ребенка за последнее время;

Соберите наиболее полную информацию о происшествии, как со слов ребенка, так и спомощью технических средств- зайдите на станицы сайта, где был ваш ребенок, посмотрите список его друзей, прочтите сообщения.

 При необходимости скопируйте и сохраните эту информацию-в дальнейшем это может вам пригодиться.

Если вы не уверенны в оценке серьезности произошедшего с вашим ребенком, или ребенок недостаточно откровенен с вами или вообще не готов идти на контакт, или вы не знаете как поступить в той или иной ситуации - обратитесь к специалисту, где вам дадут рекомендации о том, куда и в какой форме обратиться, если требуется вмешательство других служб и организации .

**Общие рекомендации по обеспечению безопасности детей и подростков в**

**Интернете**

1.Расположите компьютер вашего ребенка в месте общей доступности: столовой ли гостиной. Так вам будет проще уследить за тем, что делают дети в интернете.

2.Следите, какие сайты посещают ваши дети. Если у вас маленькие дети, знакомьтесь с интернетом вместе. Если у вас дети постарше, поговорите с ними о сайтах, которые они посещают, и осудите, что допустимо, а что недопустимо в вашей семье. Список сайтов, которые посещают ваш ребенок, можно найти в истории браузера. Кроме того, вы можете воспользоваться инструментами блокировки нежелательного контекста, такими как, например, безопасный поиск Google или безопасный режим на YouTube.

3.Раскажите детям о безопасности в интернете. Вы не сможете все время следить за теми, что ваши дети делают в сети. Им необходимо научиться самостоятельно пользоваться интернетом безопасным и ответственным образам.

4. Установите защиту от вирусов. Используйте и регулярно обновляйте антивирусное ПО. Научите детей не загружать файлы с файлообменных сайтов, а также не принимать файлы и не загружать вложения, содержащие в электронных письмах от незнакомых людей.

5.Научите детей ответственному поведению в интернете. Помните золотое правило; то, что вы не сказали бы человеку в лицо, не стоит отправлять ему по MS, электронной почте, чате или размещать в комментариях на его странице в сети.

6.Оценивайте интернет-контент критически. То, что содержится в интернете, не всегда правда. Дети должны научиться отличать надежные источники информации от ненадежных и проверять информацию, которую они находят в интернете. Также объяснить детям, что копирование и вставка содержимого с чужих веб-сайтов могут быть признаны плагиатом.

7. Если нуждаетесь в консультации специалиста по вопросом безопасного использования интернета или если ваш ребенок уже столкнулся с рисками в сети, обратитесь к специалистам за помощью.

Пять правил безопасности пользования электронной почтой:

1. Никогда не открывайте подозрительные сообщения или вложения электронной почты, полученные от незнакомых людей. Вместо этого удалите их, выбрав команду в меню сообщения.

2. Никогда не отвечайте на спам.

3. Применяйте фильтр спама поставщика услуг интернета или программы работы с электронной почтой .

4.Создайте новый или используемый семейный адрес электронной почты для интернет-запросов, дискуссионных форумов и т.д.

5.Никогда не пересылайте «письма счастья».Вместо этого сразу удаляйте их.